Universität Paderborn
INSTITUT FÜR MATHEMATIK
Dr. Job Kuit

Sommersemester 2024

Lineare Algebra für Informatiker

2. Übungsblatt - Lösungen

Präsenzaufgabe 2.1 Sei $(G, \star)$ eine Gruppe. Beweisen Sie die folgenden Aussagen.

(a) Wenn $x^2 = e$ für alle $x \in G$ dann ist G abelsch.
Lösung: Seien $x, y \in G$. Es gilt $x \star y \star x \star y = (x \star y)^2 = e$. Weil $x^2 = y^2 = e$, folgt

$$y \star x = e \star y \star x \star e = x^2 \star y \star x \star y^2 = x \star (x \star y \star x \star y) \star y = x \star e \star y = x \star y.$$

(b) G ist genau dann abelsch, wenn die Abbildung $\iota : G \to G$, $x \mapsto x^{-1}$ ein Gruppenhomomorphismus ist.
Lösung: Für alle $x, y \in G$ gilt $(x \star y)^{-1} = y^{-1} \star x^{-1}$ und $(x^{-1})^{-1} = x$.

Nehme an, dass G abelsch ist. Dann gilt für alle $x, y \in G$

$$\iota(x \star y) = (x \star y)^{-1} = y^{-1} \star x^{-1} = x^{-1} \star y^{-1} = \iota(x) \star \iota(y)$$

Für die dritte Gleichung haben wir verwendet, dass G abelsch ist. Es folgt, dass ι ein Gruppenhomomorphismus ist.

Nehme jetzt an, dass ι ein Gruppenhomomorphismus ist. Seien $x, y \in G$. Es gilt

$$\begin{aligned} x \star y &= \big((x \star y)^{-1}\big)^{-1} = \big(y^{-1} \star x^{-1}\big)^{-1} = \iota\big(y^{-1} \star x^{-1}\big) = \iota(y^{-1}) \star \iota(x^{-1}) \\ &= (y^{-1})^{-1} \star (x^{-1})^{-1} = y \star x. \end{aligned}$$

Für die vierte Gleichung haben wir verwendet, dass ι ein Gruppenhomomorphismus ist. Es folgt, dass G abelsch ist.

Präsenzaufgabe 2.2 Sei $(R, +, \cdot)$ ein Ring. Sei

$$R^\times := \{x \in R : \text{ es gibt ein } y \in R, \text{ sodass } x \cdot y = y \cdot x = 1\}.$$

(Die Elemente in $R^\times$ heißen Einheiten.)

(a) Beweisen Sie, dass $(R^\times, \cdot)$ eine Gruppe ist.
Lösung:

0. Seien $x_1, x_2 \in R^\times$. Es gibt $y_1, y_2 \in R$, sodass

$$x_1 \cdot y_1 = y_1 \cdot x_1 = 1 \quad \text{und} \quad x_2 \cdot y_2 = y_2 \cdot x_2 = 1.$$

Es gilt

$$(x_1 \cdot x_2) \cdot (y_2 \cdot y_1) = x_1 \cdot \big(x_2 \cdot y_2\big) \cdot y_1 = x_1 \cdot 1 \cdot y_1 = x_1 \cdot y_1 = 1$$

und

$$(y_2 \cdot y_1) \cdot (x_1 \cdot x_2) = y_2 \cdot (y_1 \cdot x_1) \cdot x_2 = y_2 \cdot 1 \cdot x_2 = y_2 \cdot x_2 = 1.$$

Es folgt, dass $x_1 \cdot x_2 \in R^\times$.

1. Multiplikation in R ist assoziativ.
2. Das neutrale Element für Multiplikation $1 \in R$ ist enthalten in $R^\times$, denn $1 \times 1 = 1$.
3. Sei $x \in R^\times$. Nach Definition gibt es ein $y \in R$ mit $x \cdot y = y \cdot x = 1$, d.h. y ist eine multiplikative Inverse von x. Es gilt $y \in R^\times$, denn $y \cdot x = x \cdot y = 1$.

(b) Bestimmen Sie $R^\times$, falls $R = \mathbb{Z}/20\mathbb{Z}$.
Lösung: Wenn $x \in R^\times$, dann gibt es ein $y \in R$, sodass $x \cdot y = y \cdot x = 1$. Für alle $z \in R \setminus \{0\}$ gilt

$$(z \cdot x) \cdot y = z \cdot (x \cdot y) = z \cdot 1 = z \neq 0$$

Wenn $z \cdot x$ gleich 0 wäre, dann $(z \cdot x) \cdot y = 0$. Es folgt, dass $x \cdot z \neq 0$ für alle $z \in R \setminus \{0\}$.

Sei $n \in \mathbb{Z}$. Wenn n teilbar durch 2 ist, dann ist $10n$ teilbar durch 20 und darum $[10][n] = [0]$. Ebenso , wenn n teilbar durch 5 ist, dann ist $4n$ teilbar durch 20 und darum $[4][n] = [0]$. Darum gilt

$$R^\times \subseteq \{[n] \in \mathbb{R} : n \text{ ist nicht teilbar durch 2 oder 5}\} = \{[1], [3], [7], [9], [11], [13], [17], [19]\}.$$

Es gilt

$$\begin{aligned}
&[1][1] = [1],\\
&[3][7] = [7][3] = [21] = [1],\\
&[9][9] = [81] = [1],\\
&[11][11] = [121] = [1],\\
&[13][17] = [17][13] = [221] = [1],\\
&[19][19] = [361] = [1]
\end{aligned}$$

und darum

$$R^\times = \{[1], [3], [7], [9], [11], [13], [17], [19]\}.$$

Präsenzaufgabe 2.3 Der fermatsche Primzahltest ist ein Primzahltest, der auf dem kleinen fermatschen Satz beruht. Sei $n \in \mathbb{N}$ mit $n \geq 2$. Wähle ein $a \in \mathbb{Z}$. Wenn $[a]^{n-1} \neq [1]$, dann ist n keine Primzahl. Sonnst könnte n eine Primzahl sein.
Betrachten Sie $n = 57$ und berechnen Sie $[2]^{56}$. Zeigen Sie damit, dass 57 keine Primzahl ist.
Lösung: Es gilt

$$\begin{aligned}
&[2]^6 = [2^6] = [64] = [7],\\
&[2]^{12} = [7]^2 = [49] = [-8],\\
&[2]^{24} = [-8]^2 = [64] = [7],\\
&[2]^{48} = [7]^2 = [49] = [-8]
\end{aligned}$$

und damit

$$[2]^{56} = [2]^{48}[2]^6[2]^2 = [-8][7][4] = [-56][4] = [1][4] = [4] \neq [1].$$

Es folgt, dass 57 nicht prim ist.

Präsenzaufgabe 2.4 Bestimmen Sie $q(x), r(x) \in \mathbb{R}[x]$, sodass

$$f(x) = q(x)g(x) + r(x) \quad \text{und} \quad \deg(r(x)) < \deg(g(x)),$$

wobei $f(x), g(x) \in \mathbb{R}[x]$ gegeben werden durch

(a) $f(x) = x^6 - x^4 + 2x^2 + 1$ und $g(x) = x^2 + 1$,
Lösung: Es gilt

$$
\begin{aligned}
x^6 - x^4 + 2x^2 + 1 &= x^4(x^2+1) + \big(- 2x^4 + 2x^2 + 1\big) \\
&= x^4(x^2+1) - 2x^2(x^2+1) + \big(4x^2+1\big) \\
&= x^4(x^2+1) - 2x^2(x^2+1) + 4(x^2+1) - 3 \\
&= \big(x^4 - 2x^2 + 4\big)(x^2+1) - 3
\end{aligned}
$$

und darum $f(x) = q(x)g(x) + r(x)$ mit $q(x) = x^4 - 2x^2 + 4$ und $r(x) = -3$. Bemerke, dass $\deg(r(x)) = 0 < 2 = \deg(g(x))$.

(b) $f(x) = 7x^8 - x^2$ und $g(x) = x^3 - 1$.
Lösung: Es gilt

$$
\begin{aligned}
7x^8 - x^2 &= 7x^5(x^3-1) + \big(7x^5 - x^2\big) \\
&= 7x^5(x^3-1) + 7x^2(x^3-1) + 6x^2 \\
&= \big(7x^5 + 7x^2\big)(x^3-1) + 6x^2
\end{aligned}
$$

und darum $f(x) = q(x)g(x) + r(x)$ mit $q(x) = 7x^5 + 7x^2$ und $r(x) = 6x^2$. Bemerke, dass $\deg(r(x)) = 2 < 3 = \deg(g(x))$.